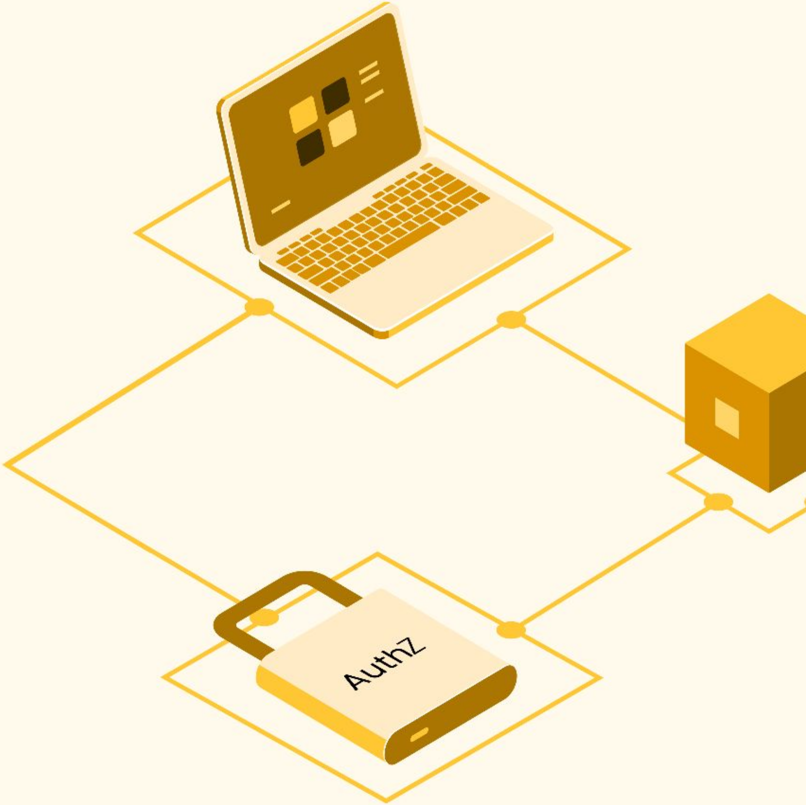
Patterns of failure in modern auth

Dan “ *phrawzty* ” Maher

cerbos



Context: About me

- Recovering system administrator
- Secretly French (🤫 don’t tell anybody)
- Frequently at lunch with the security folks at Datadog
- Currently work on open source at a start-up called Cerbos

Context: About Cerbos

- *"Externalized, policy-based, runtime authorization for your applications"*
- It's literally a self-hosted binary with an HTTP API
- There's also a hub with a bunch of neat features
- Open source (we're a Go shop)

What is authorization?

What is authorization?

- *“Is this entity allowed to perform this action on this resource?”*
- Related to, but distinct from, authentication (which is also very important!)

Early days: POSIX permissions

- User / Group / World model
- Read / Write / Execute primitives

ℹ️ *IEEE Std 1003.1 ™-2017 (Revision of IEEE Std 1003.1-2008): https://pubs.opengroup.org/onlinepubs/9699919799/*

The middle ages: ACLS & RBAC

- Access Control Lists
- Role-Based Access Control

ℹ️ *Rationale for the RBAC96 family of access control models: https://dl.acm.org/doi/10.1145/270152.270167*
ℹ️ *Proposed NIST standard for role-based access control: https://dl.acm.org/doi/10.1145/501978.501980*

Modern authorization (and authentication too!)

- Token-based approaches (JWT, OIDC)
- Federated systems
- PBAC, ABAC, ReBAC…

ℹ️ *IETF 7519 JSON Web Token (JWT): https://datatracker.ietf.org/doc/html/rfc7519*
ℹ️ *OpenID Connect Core 1.0 [2023]: https://openid.net/specs/openid-connect-core-1_0.html*

When it all goes wrong

Facebook "Privacy bug": Overview

- 📆 May 2018
- Audience selector default changed to public
- 14 million users affected
- Policy enforcement failure during feature update

ℹ️ *Data Protection Commission (Ireland):*
https://www.dataprotection.ie/sites/default/files/uploads/2022-09/Full%20Decision%2018-11-5%20Facebook%2012%20breaches.pdf

Facebook "Privacy bug": Key auth failures

- Default permission setting changed without user consent
- Policy enforcement layer failed during UI update
- Inadequate permission state validation

ℹ️ *Privacy by Design: A Counterfactual Analysis […]: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2128146*

Okta "Support system breach": Overview

- 📅 October 2023
- HAR file exfiltration exposed session tokens
- Auth bypasses in support systems

ℹ️ *Okta October 2023 Security Incident Investigation Closure: https://sec.okta.com/articles/harfiles/*

Okta "Support system breach": Key auth failures

- Overly permissive access to production
- Insufficient isolation between support tiers
- Authorization checks bypassed through session token theft
- Inadequate token validation controls

ℹ️ *BeyondTrust Discovers Breach of Okta Support Unit:* [*https://www.beyondtrust.com/blog/entry/okta-support-unit-breach*](https://www.beyondtrust.com/blog/entry/okta-support-unit-breach)

Microsoft "Midnight Blizzard": Overview

- 📆 Late 2023 / early 2024
- Password spray attack led to tenant compromise
- Legacy tenants, basic auth, and privilege escalation

ℹ️ *Midnight Blizzard: Guidance for responders on nation-state attack:*
https://www.microsoft.com/en-us/security/blog/2024/01/25/midnight-blizzard-guidance-for-responders-on-nation-state-attack/

Microsoft "Midnight Blizzard": Key auth failures

- Excessive privileges in legacy tenant configurations
- Inadequate role separation
- Authorization boundaries between tenants insufficiently enforced
- Lack of just-in-time access controls for privileged operations

ℹ️ *Office of Information Security (HHS) report 202411131500:*
https://www.hhs.gov/sites/default/files/new-midnight-blizzard-campaign-analyst-note-tlpclear.pdf

How to stop it all from going wrong

Token Security

- Validation best practices (signature, expiry, issuer)
- Secure storage and transport
- Avoiding common token vulnerabilities

ℹ️ *IETF RFC 8725 JSON Web Token Best Current Practices: https://datatracker.ietf.org/doc/html/rfc8725*
ℹ️ *Vaadata JWT Vulnerabilities, Common Attacks, & Best Practices:*
https://www.vaadata.com/blog/jwt-json-web-token-vulnerabilities-common-attacks-and-security-best-practices/

Permission Management

- Role explosion 💥
- Real-time or JIT access patterns
- Principle of least privilege

ℹ️ *OWASP Authorization Cheat Sheet:* [*https://cheatsheetseries.owasp.org/cheatsheets/Authorization_Cheat_Sheet.html*](https://cheatsheetseries.owasp.org/cheatsheets/Authorization_Cheat_Sheet.html)
ℹ️ *NIST Zero Trust Architecture (2020):* [*https://www.nist.gov/publications/zero-trust-architecture*](https://www.nist.gov/publications/zero-trust-architecture)

Externalizing Authorization

- Clear separation between business logic and authz rules
- Update policies without updating code
- Enhanced auditability and compliance reporting

ℹ️ *CNCF 5 laws of cloud native authz: https://www.cncf.io/blog/2023/01/19/the-five-laws-of-cloud-native-authorization/*
ℹ️ *Cerbos What is EAM?: https://www.cerbos.dev/blog/externalized-authorization-management-eam-and-benefits*

Testing Auth Systems

- Specific analysis
- Policy unit testing
- Automated access review

ℹ️ *OWASP Authentication Testing*:
https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/04-Authentication_Testing/README
ℹ️ *OWASP Authorization Testing*:
https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/05-Authorization_Testing/README

Critical Path Patterns

- High-availability authorization
- Graceful degradation strategies
- When in doubt, deny by default

ℹ️ *CNCF Cloud Native Security Whitepaper:*
https://www.cncf.io/wp-content/uploads/2022/06/CNCF_cloud-native-security-whitepaper-May2022-v2.pdf
ℹ️ *Netflix Edge Authentication and Token-Agnostic Identity Protection:*
https://netflixtechblog.com/edge-authentication-and-token-agnostic-identity-propagation-514e47e0b602

Conclusion

- Authorization fails at boundaries and transitions
- **Externalize your authorization decisions**
- Tokens require rigorous validation
- Use real-time access patterns and live the principle of least privilege
- Test continuously and review access regularly

I just met you
and this is crazy
but here’s my QR
so Cerbos maybe?

Thanks!